On Factorisations of Matrices and Abelian Groups.

Johan Andersson* and Gautami Bhowmik†

February 2, 2008

Abstract

We establish correspondances between factorisations of finite abelian groups (direct factors, unitary factors, non isomorphic subgroup classes) and factorisations of integer matrices. We then study counting functions associated to these factorisations and find average orders.

Mathematics Subject Classification 11M41,20K01,15A36.

1 Introduction

In this paper we study the correspondance between different factorisations of finite abelian groups and that of integer matrices. In particular, we are interested in the matter of enumeration. This is in line with the questions on direct and unitary factors of abelian groups first raised by Cohen [Coh60] in 1960 and subgroups of abelian groups studied since long in different contexts (see, eg, Butler [But87], Goldfeld-Lubotzky-Pyber [GLP04] or Bhowmik-Ramare [BR98]).

We consider the decomposition of a finite abelian group G as a direct sum

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_1n_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_1n_2\cdots n_r\mathbb{Z}$$

where n_i are divisors of the *order* $n = n_1^r n_2^{r-1} \cdots n_r$ and r the *rank* of the group. In terms of integer matrices this group can be associated to a canonical representative of a double coset

$$M(G) = diag[n_1, n_1n_2, \cdots, n_1n_2\cdots n_r].$$

*Department of Mathematics, Stockholm University, SE-106 91 Stockholm, Sweden. Email : johana@math.su.se

†Université de Lille 1, UMR CNRS 8524, 59655 Villeneuve d'Ascq Cedex, France. Email : bhowmik@math.univ-lille1.fr

The matrix $M(G)$ is said to be in *Smith Normal Form* (SNF) or sometimes an elementary divisor and its determinant equals the order of the group G. It is well known that the number of non-isomorphic abelian groups of order upto x is asymptotic to Lx [ES34] where L is a constant. If the rank is bounded by r, this corresponds to the number of $r \times r$ SNF matrices of determinant upto x and then the constant depends on r [Bho93].

In 1960 E. Cohen [Coh60] defined the factorization of finite abelian groups as a decomposition in formal direct factors. He introduced the zeta function associated to the direct factorization, $G = H \oplus K$, and obtained that the number of direct factors, on an average, is $\log x$. In Section 1 we interpret direct factorisations of G in terms of decompositions into SNF factors of the 'conjugate' matrix of G. The idea of conjugate matrices comes from considering the type of a group, in the sense of Macdonald [Mac79]. Thus we can treat the truncated zeta function

$$\zeta^2(s)\zeta^2(2s)\zeta^2(3s)\cdots\zeta^2(rs)$$

as a counting function of certain direct factors of abelian groups. The case of unitary factorisations is treated similarly.

Later, [BR98] it was proved that a subgroup of G corresponds to a divisor of $M(G)$ which is a canonical representative of a right coset, for example a matrix in *Hermite Normal Form* (HNF). Using the zeta function associated to subgroups it was found that on an average there were many more subgroups than direct factors. The number of subgroups of an abelian group is essentially $x^{([r^2/4]+1)/r-1}$, which is heavily dependent on the rank.

In Section 2 we consider classes of subgroups under isomorphism. In terms of matrices we are interested in divisors of $M(G)$ which are in SNF. We now investigate whether on an average the number of non-isomorphic subgroups depends on the rank of the group.

To do so we introduce the zeta function

$$Z_r(s) = \sum_{n=0}^{\infty} A_r(n) n^{-s}$$

where $A_r(n)$ denotes the number of subgroup classes (under isomorphism) of abelian groups of order n rank atmost r and use this function to get the mean value

$$\sum_{n=1}^{x} A_r(n) \sim C_r x \log x$$

for positive integers r. This shows that on an average the number of non-isomorphic subgroups is about the same as the number of direct factors whereas the number of all subgroups is much larger as the rank increases. The same average order holds true when we consider subgroups of arbitrary rank.

While $Z_r(s)$ in general have no global functional equation we will prove that for all positive integers r it has a local functional equation

$$Z_r(s) = \prod_{p \text{ prime}} F_r(p^{-s}),$$

with

$$F_r(x) = x^{-r(r+3)/2} F_r\left(\frac{1}{x}\right).$$

This follows from a recursion formula that we develop for the functions $F_r(x)$. We include some values of the generating function by using this recursion formula, the first few being

$$Z_1(s) = \zeta^2(s), \quad Z_2(s) = \frac{\zeta^2(s)\zeta^3(2s)}{\zeta(3s)} \quad \text{and} \quad Z_3(s) = \frac{\zeta^2(s)\zeta^3(2s)\zeta^3(3s)}{\zeta(4s)} G(s),$$

where $G(s)$ is a Dirichlet series absolutely convergent for $\mathrm{Re}(s) > 1/5$.

For the limit case $Z(s) = \lim_{r\to\infty} Z_r(s)$ we show that while $Z(s)$ does have a meromorphic continuation to $\mathrm{Re}(s) > 0$, it does not have a meromorphic continuation beyond the imaginary axis. We tend to believe that the same is true for $Z_r(s)$ when $r \geq 3$.

Acknowledgement. *The second author thanks Radoslav Dimitriç for useful discussions.*

2 Direct Factors.

In this section we discuss the relationship between direct factors of abelian groups and factorisation of matrices. We recall a definition.

Definition 1. An abelian group G has a (formal) *direct factorisation* into H and K, noted as $G = H \oplus K$ if $G = H + K$, H and K being subgroups of G whose only intersection as subgroups is trivial.

Formal direct factors of abelian groups were studied in the context of arithmetic functions of abelian groups and Cohen [Coh60] defined direct Dirichlet convolution of abelian groups in terms of this decomposition, i.e.

$$(\chi_1 * \chi_2)(G) = \sum_{G=H\oplus K} \chi_1(H)\chi_2(K),$$

where χ_i are arithmetical functions of abelian groups, in an attempt to generalise the factorisation of integers.

With no loss of generalisation, we can consider p-groups, i.e.

$$G_p \cong \mathbb{Z}/p^{a_1}\mathbb{Z} \oplus \mathbb{Z}/p^{a_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{a_r}\mathbb{Z},$$

where the order of G_p is $p^{a_1+a_2+\cdots+a_r}$, for a prime number p and $0 \leq a_1 \leq a_2 \leq \cdots \leq a_r$.

The invariants of G is given by the partition $\lambda = (a_1, a_2, \cdots, a_r)$, which, in combinatorics, is called the *type* of G. We call the group whose type λ' is the conjugate of λ, the *conjugate of* G and denote it by G'. We now express the direct factorisation above as a matrix factorisation.

Definition 2. The *SNF factorisation* of a SNF matrix S is a decomposition into SNF matrices whose product equals S.

We now establish the following bijection

Proposition 1. *If $M(G') = M(H')M(K')$ is a SNF factorisation, then $G = H \oplus K$ is a direct factorisation and conversely.*

Proof. Let G be a group of type

$$\lambda = (\underbrace{f_1}_{g_1 \text{ times}}, \underbrace{f_1+f_2}_{g_2 \text{ times}}, \ldots, \underbrace{f_1+f_2+\cdots+f_m}_{g_m \text{ times}}).$$

Then

$$\lambda' = (\underbrace{g_m}_{f_m \text{ times}}, \underbrace{g_m+g_{m-1}}_{f_{m-1} \text{ times}}, \ldots, \underbrace{g_m+g_{m-1}+\cdots+g_1}_{f_1 \text{ times}}).$$

Writing $g_i = h_i + k_i$, sum of non-negative integers, we get types of groups H' and K' such that $M(G') = M(H')M(K')$ is a SNF factorisation, i.e.

$$M(H') = diag[\underbrace{p^{h_m}, \ldots, p^{h_m}}_{f_m \text{ times}}, \underbrace{p^{h_m+h_{m-1}}, \ldots}_{f_{m-1} \text{ times}}, \ldots, \underbrace{p^{h_m+h_{m-1}+\cdots+h_1}}_{f_1 \text{ times}}]$$

etc. whereas

$$H \cong \oplus_{h_1}\mathbb{Z}/p^{f_1}\mathbb{Z} \oplus_{h_2} \mathbb{Z}/p^{f_1+f_2}\mathbb{Z} \cdots \oplus_{h_m} \mathbb{Z}/p^{f_1+f_2+\cdots+f_m}\mathbb{Z}$$

and

$$K \cong \oplus_{k_1}\mathbb{Z}/p^{f_1}\mathbb{Z} \oplus_{k_2} \mathbb{Z}/p^{f_1+f_2}\mathbb{Z} \cdots \oplus_{k_m} \mathbb{Z}/p^{f_1+f_2+\cdots+f_m}\mathbb{Z},$$

where $\oplus_t$ before a summand means that it is repeated t times.

Thus the type of H is

$$(\underbrace{f_1}_{h_1 \text{ times}}, \underbrace{f_1+f_2}_{h_2 \text{ times}}, \ldots, \underbrace{f_1+f_2+\cdots+f_m}_{h_m \text{ times}})$$

and that of K is

$$(\underbrace{f_1}_{k_1 \text{ times}}, \underbrace{f_1+f_2}_{k_2 \text{ times}}, \ldots, \underbrace{f_1+f_2+\cdots+f_m}_{k_m \text{ times}}),$$

and the relation $G \cong H \oplus K$ is satisfied.

The converse is proved by taking $G \cong H \oplus K$ as above and retracing the steps. □

Example 1. Let $G \cong \mathbb{Z}/p^2\mathbb{Z} \oplus \mathbb{Z}/p^2\mathbb{Z} \oplus \mathbb{Z}/p^4\mathbb{Z}$. Here $\lambda = (2, 2, 4)$, thus the conjugate $\lambda' = (1, 1, 3, 3)$. The following non-trivial SNF factorisations of $M(G')$, i.e.

$$M(G') = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & p & 0 \\ 0 & 0 & 0 & p \end{pmatrix} \begin{pmatrix} p & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & p^2 & 0 \\ 0 & 0 & 0 & p^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & p^2 & 0 \\ 0 & 0 & 0 & p^2 \end{pmatrix} \begin{pmatrix} p & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & p & 0 \\ 0 & 0 & 0 & p \end{pmatrix}$$

give $H \cong \mathbb{Z}/p^2\mathbb{Z}, K \cong \mathbb{Z}/p^2\mathbb{Z} \oplus \mathbb{Z}/p^4\mathbb{Z}$ and $H \cong \mathbb{Z}/p^2\mathbb{Z} \oplus \mathbb{Z}/p^2\mathbb{Z}, K \cong \mathbb{Z}/p^4\mathbb{Z}$. Obviously, changing the order of the matrices would interchange H and K.

The generating function for the number of direct factors of a finite abelian group is given by

$$\mathcal{D}(s) = \zeta^2(s)\zeta^2(2s)\zeta^2(3s)\cdots$$

as was first done by Cohen [Coh60] and subsequently studied by many, for example Krätzel [Krä88], Menzer [Men95], Wu [Wu00] or Knopfmacher [Kno85].

A truncated form of this function,

$$\mathcal{D}_r(s) = \zeta^2(s)\zeta^2(2s)\zeta^2(3s)\cdots\zeta^2(rs)$$

occurs as the Dirichlet series associated to the SNF factorisation of an $r \times r$ integer matrix, see, for example [Bho93], which we can now interpret in the context of abelian groups:

Theorem 1. *The function $\zeta^2(s)\zeta^2(2s)\zeta^2(3s)\cdots\zeta^2(rs)$ generates the direct factors of finite abelian groups whose conjugates have rank atmost r.*

This implies the following result on average orders:

Corollary 1. *The number of direct factors of non-isomorphic abelian groups of order atmost x whose conjugates have rank atmost r is asymptotic to $A_r x \log x$, where A_r is a constant that depends on r.*

3 Unitary Factors.

Unitary factors of finite abelian groups were also studied by Cohen as a generalisation of the corresponding idea on integers, where one encounters the function

$$t(n) = \sum_{d|n,\ gcd(d,n/d)=1} 1.$$

Definition 3. An abelian group G has unitary factors H and K if $G \cong H \oplus K$ is a direct factorisation H and K have no further common direct factor.

As above, we see that in terms of matrices this corresponds to block SNF factorisations, i.e. for $M(G')$ as above, $M(H')$ is a unitary factor if h_i is either 0 or g_i for each i. Thus the number of unitary factors of G is 2^m.

Example 2. With G as in Example 1, the only non-trivial unitary factorisation $H \cong \mathbb{Z}/p^2\mathbb{Z} \oplus \mathbb{Z}/p^2\mathbb{Z}, K \cong \mathbb{Z}/p^4\mathbb{Z}$ corresponds to the SNF factorisation

$$M(G') = \begin{pmatrix} pI_2 & 0 \\ 0 & p^3 I_2 \end{pmatrix} = \begin{pmatrix} I_2 & 0 \\ 0 & p^2 I_2 \end{pmatrix} \begin{pmatrix} pI_2 & 0 \\ 0 & pI_2 \end{pmatrix},$$

where I_2 is the 2×2 identity matrix.

The level function $u_r(n)$ that counts the number of unitary factors of abelian groups of order n whose conjugates have rank atmost r is given by

$$u_r(n) = \sum_{n=n_1^r n_2^{r-1} \ldots n_r} 2^{\omega(n_1)+\omega(n_2)+\cdots+\omega(n_r)},$$

where $\omega(n)$ gives the number of distinct prime factors of n. We obtain

Theorem 2. *The associated zeta function*

$$\mathcal{U}_r(s) = \sum_{n=1}^{\infty} u_r(n) n^{-s}$$

can be written as

$$\mathcal{U}_r(s) = \frac{\zeta^2(s)\zeta^2(2s)\zeta^2(3s)\cdots\zeta^2(rs)}{\zeta(2s)\zeta(4s)\zeta(6s)\cdots\zeta(2rs)}.$$

This implies the following result on average orders:

Corollary 2. *The number of unitary factors of finite abelian groups of order atmost x whose conjugates have rank atmost r is asymptotic to $K_r x \log x$, where K_r is a constant that depends on r.*

In the infinite dimensional case, the study of the average order first occurs in literature at the same time as direct factors and continues to be refined. (See, eg. Calderón [Cal03] or Zhai [Zha00]).

4 Subgroup Classes

It is easy to see that the number of classes of subgroups of G corresponds to the number of divisors of $M(G)$ which are themselves in SNF. Thus we are interested in the function

$$\sum_{M_1|M(G),\ M_1\ \ SNF} 1 = \sum_{H<G} 1,$$

where for all isomorphic subgroups H, we count only once. For our purpose it is enough to consider a p-group

$$G_p \cong \mathbb{Z}/p^{a_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{a_1+\cdots+a_r}\mathbb{Z}$$

whose type is the partition $(a_1, a_1+a_2, \ldots, a_1+\cdots+a_r)$, $a_i \geq 0$. We wish to count all subgroups H whose type is "less than" the type of G, i.e. where the type of H is $(b_1, b_1+b_2, \ldots, b_1+\cdots+b_r)$ with $\sum_{i=1}^{j} b_i \leq \sum_{i=1}^{j} a_i$, for $1 \leq j \leq r$.

Thus we study the function

$$f_r(a_1, a_2, \ldots, a_r) = \sum_{b_1=0}^{a_1} \sum_{b_2=0}^{a_1+a_2-b_1} \cdots \sum_{b_r=0}^{a_1+a_2+\cdots+a_r-b_1-b_2-\cdots-b_{r-1}} 1. \tag{1}$$

Collecting the exponents $ra_1+\cdots+a_r = k$, we write

$$F_r(x) = \sum_{k=0}^{\infty} \alpha_r(k) x^k, \tag{2}$$

where

$$\alpha_r(k) = \sum_{ra_1+\cdots+a_r=k} f_r(a_1, a_2, \ldots, a_r). \tag{3}$$

Now let $c_j = a_1+\cdots+a_j$ and $d_j = b_1+\cdots+b_j$ and let $\lambda_k = (c_1, c_2, \cdots, c_r)$ and $\mu_m = (d_1, d_2, \cdots, d_r)$ be partitions of k and $m \leq k$ respectively. Then $\alpha_r(k)$ denotes the number of pairs of partitions $\{(\lambda_k, \mu_m)\}$, such that $d_i \leq c_i$.

We first obtain a recursion formula for the $\alpha_r(k)$. To do so directly seems difficult, and it is convenient to introduce an additional parameter j.

Definition 4. Let $\alpha_r(k,j)$ be defined as $\alpha_r(k)$, but where the condition $0 \leq d_1 \leq \cdots \leq d_r$ is replaced by $-j \leq d_0 \leq d_1 \leq \cdots \leq d_r$, i.e.

$$\alpha_r(k,j) = \sum_{\substack{c_1+\cdots+c_r=k \\ 0\leq c_1\leq\cdots\leq c_r}} \sum_{d_0=-j}^{0} \sum_{d_1=d_0}^{c_1} \sum_{d_2=d_1}^{c_2} \cdots \sum_{d_r=d_{r-1}}^{c_r} 1. \tag{4}$$

Proposition 2. *One has the recursion formula*

$$(i) \qquad \alpha_0(k,j) = \begin{cases} j+1, & k=0, \\ 0, & k \geq 1. \end{cases}$$

$$(ii) \qquad \alpha_r(k,-j) = 0, \qquad j \geq 1.$$

$$(iii) \qquad \alpha_r(k,j) = \alpha_r(k,j-1) + \sum_{m=0}^{[k/r]} \alpha_{r-1}(k-mr, m+j), \qquad (r \geq 1, j \geq 0).$$

$$(iv) \qquad \alpha_r(k,0) = \alpha_r(k).$$

Proof. Equations $(i), (ii)$ and (iv) follow from Definition 4.

For (iii), the condition $-j \leq d_0$ in Definition 4 can be divided into two cases, either $-(j-1) \leq d_0$ from which we get the contribution $\alpha_r(k, j-1)$, in (iii) ; or $d_0 = -j$ in which case we let $c_1 = m$ and denote

$$c'_i = c_{i+1} - m, \qquad \text{and} \qquad d'_i = d_{i+1} - m.$$

It is clear that $(0, c'_1, c'_2, \cdots \leq c'_{r-1})$ is a partition of $k - mr.$, while $d'_0 \leq 0$, $-m-j \leq d'_0 \leq d'_1 \leq \cdots \leq d'_{r-1}$, and $d'_j \leq c'_j$. We thus get a contribution

$$\alpha_{r-1}(k - mr, m + j)$$

for each $0 \leq m \leq [k/r]$, and this concludes the proof of (iii). □

We introduce the notation $\alpha(k) = \alpha_k(k)$.

Since the number of partitions of k into k non-zero parts is equal to the number of partitions of k into r parts, $r > k$, we get,

$$\alpha_r(k) = \alpha(k). \qquad (r \geq k) \tag{5}$$

Thus,

$$\lim_{r \to \infty} \alpha_r(k) = \alpha(k)$$

We now obtain some simple bounds in terms of the classical partition function.

Lemma 1. *We have that*

$$q(k) \leq \alpha(k) \leq kq(k)^2,$$

where $q(n)$ denotes the total number of partitions of the n.

Proof. The lower bound follows from the definition. Now let $\lambda_k = (c_1, c_2, \cdots, c_k)$ and $\lambda_m = (d_1, d_2, \cdots, d_k)$ be partitions of k and $m \leq k$ respectively. If $d_1 \neq 0, \lambda_m$ can be completed to $(1, \cdots, 1, d_1, d_2, \cdots, d_k)$, a partition of k. There are atmost $q(k)$ of such λ_m.

If $d_1 = 0, d_2 \neq 0$, we can complete λ_m to get a partition of $k - c_1$. In this way, for each λ_m we have atmost

$$q(k) + q(k - c_1) + \cdots + q(k - c_k) \leq kq(k)$$

possibilities. Since there are $q(k)$ ways to write λ_k, the upper bound follows. $\square$

We will now turn our attention to the generating functions

Definition 5. Let $\alpha_r(k), \alpha_r(k, j)$, and $\alpha(k)$ be as above. We define the generating functions to be

$$F_r(x) = \sum_{k=0}^{\infty} \alpha_r(k) x^k,$$

$$F_r(x, y) = \sum_{k,j=0}^{\infty} \alpha_r(k, j) x^k y^j,$$

and

$$F(x) = \sum_{k=0}^{\infty} \alpha(k) x^k.$$

These definitions are consistent, since

$$F_r(x) = F_r(x, 0), \tag{6}$$

the only term that survives with $y = 0$ is when $j = 0$.

Lemma 2. *With F and F_r defined as above one has that $F(x)$ and $F_r(x)$ are analytic functions in the unit disc with integer power series coefficients such that $F(0) = F_r(0) = 1$. Furthermore the function F satisfies the inequality*

$$F(x) \geq \frac{1}{\prod_{k=1}^{\infty}(1 - x^k)}. \qquad (0 < x < 1)$$

Proof. The power series coefficients of F_r and F are integers since they are counting functions and by Proposition 2 (i) and (iv) and eq. (5), we have that $\alpha_r(0) = 1$ and $\alpha(0) = 1$, which implies $F_r(0) = F(0) = 1$. By the well known generating function for the classical partition function

$$\sum_{k=0}^{\infty} q(k) x^k = \frac{1}{\prod_{k=1}^{\infty}(1 - x^k)}, \qquad (0 < x < 1) \tag{7}$$

and the lower bound in Lemma 1

$$q(k) \leq \alpha(k),$$

this gives us the lower bound in Lemma 2. Equation (7) also implies that the generating function of the partition function is analytic in the unit disc, and hence the classical partition function $q(n)$ is of subexponential order. This implies that $k(q(k))^2$ is of subexponential order and by the upper bound in Lemma 2, so is $\alpha(n)$, and also $\alpha_r(n)$ since $0 \leq \alpha_r(n) \leq \alpha(n)$. This proves that F and F_r are analytic in the unit disc. $\square$

We will now see how the recursion formula for the coefficients $\alpha_r(k,j)$ in Proposition 2 yield a recursion formula for its generating function $F_r(x,y)$.

Proposition 3. *One has the following recursion formula for the function $F_r(x,y)$:*

$$(i) \qquad F_0(x,y) = \frac{1}{(1-y)^2},$$

$$(ii) \qquad F_r(x,y) = \frac{F_{r-1}(x,x^r)x^r - F_{r-1}(x,y)y}{(x^r-y)(1-y)}.$$

Proof. From Proposition 2 (iii) it is clear that

$$F_r(x,y)(1-y) = \sum_{k,j=0}^{\infty} \sum_{m=0}^{[k/r]} \alpha_{r-1}(k-mr, m+j)x^n y^j,$$

and by replacing k and j suitably, we get

$$\begin{aligned} F_r(x,y) - F_r(x,y)y &= \sum_{k,j=0}^{\infty} \sum_{m=0}^{j} x^{k+mr} y^{j-m} \alpha_{r-1}(k,j), \\ &= \sum_{k,j=0}^{\infty} x^k \left(\frac{x^{r(j+1)} - y^{j+1}}{x^r - y} \right) \alpha_{r-1}(k,j), \\ &= \frac{F_{r-1}(x,x^r)x^r - F_{r-1}(x,y)y}{x^r - y}. \end{aligned}$$

Proposition 2 (i) and Definition 5 give

$$\begin{aligned} F_0(x,y) &= \sum_{j=0}^{\infty} (j+1)y^j, \\ &= \frac{1}{(1-y)^2}. \end{aligned}$$

$\square$

We first notice that

Lemma 3. *The function F satisfies the identity.*

$$F_r(x) = F_{r-1}(x, x^r)$$

Proof. This follows from eq. (6) and Proposition 3 (*ii*). $\square$

We now calculate the first few values of $F_r(x)$.

Lemma 4. *One has that*

$$(i) \qquad F_0(x) = 1,$$
$$(ii) \qquad F_1(x) = (1-x)^{-2},$$

and

$$(iii) \qquad F_2(x) = (1-x)^{-2}(1-x^2)^{-3}(1-x^3).$$

Proof. Putting $y = 0$ in Proposition 3 (*i*) proves (*i*). From Lemma 3 we get that

$$F_1(x) = F_0(x, x) = \frac{1}{(1-x)^2},$$

which proves (*ii*). By Proposition 3 (*ii*) we get that

$$\begin{aligned} F_1(x, y) &= \frac{F_0(x, x)x - F_0(x, y)y}{(x-y)(1-y)} \\ &= \frac{xy - 1}{(x-1)^2(y-1)^3}. \end{aligned} \tag{8}$$

By Lemma 3 we get

$$F_2(x) = F_1(x, x^2) = \frac{x^3 - 1}{(x-1)^2(x^2-1)^3},$$

which proves (*iii*). $\square$

We further prove:

Proposition 4. *The functions $F_r(x, y)$ and $F_r(x)$ satisfy the functional equations*

$$(i) \qquad F_r(x, y) = x^{-r(r+1)/2} y^{-2} F_r\left(\frac{1}{x}, \frac{1}{y}\right),$$
$$(ii) \qquad F_r(x) = x^{-r(r+3)/2} F_r\left(\frac{1}{x}\right).$$

Proof. We will use induction to prove (i). Let $r = 0$. Proposition 3 (i) gives us that

$$\begin{aligned}
F_0(x, y) &= (1 - y)^{-2}, \\
&= y^{-2}\left(1 - \frac{1}{y}\right)^{-2}, \\
&= y^{-2} F_0\left(\frac{1}{x}, \frac{1}{y}\right), \\
&= x^{-0\cdot(0+1)/2} y^{-2} F_0\left(\frac{1}{x}, \frac{1}{y}\right),
\end{aligned}$$

and hence (i) is true for $r = 0$. We now assume that (i) is true for $r = k$. By using Proposition (3) (ii) we now obtain

$$F_{k+1}(x, y) = \frac{F_k(x, x^{k+1})x^{k+1} - F_k(x, y)y}{(x^{k+1} - y)(1 - y)},$$

Using the functional equation (i) for $r = k$ it equals

$$\begin{aligned}
&= \frac{x^{-k(k+1)/2} x^{-2(k+1)} F_k(x^{-1}, x^{-k-1})x^{k+1} - x^{-k(k+1)/2} y^{-2} F_k(x^{-1}, y^{-1})y}{(x^{k+1} - y)(1 - y)}, \\
&= x^{-(k+1)(k+2)/2} y^{-2} \frac{F_k(x^{-1}, x^{-k-1})x^{-k-1} - F_k(x^{-1}, y^{-1})y^{-1}}{(x^{-k-1} - y^{-1})(1 - y^{-1})}, \\
&= x^{-(k+1)(k+2)/2} y^{-2} F_{k+1}(x^{-1}, y^{-1}),
\end{aligned}$$

which finishes the proof for (i). We will now prove (ii). By Lemma 3 we have that

$$F_r(x) = F_{r-1}(x, x^r),$$

The functional equation with $y = x^r$ gives

$$\begin{aligned}
x^{-(r-1)r/2} x^{-2r} F_{r-1}\left(\frac{1}{x}, \frac{1}{x^r}\right), \\
= x^{-r(r+3)/2} F_r\left(\frac{1}{x}\right).
\end{aligned}$$

□

5 The zeta function of subgroup classes

5.1 The zeta function of subgroup classes of bounded rank

We will now introduce the zeta function. We use the notation $A_r(n)$ for the multiplicative function that counts the number of isomorphic subgroup classes of

abelian groups of rank less or equal to r and order n. If n is a prime power then

$$A_r(p^k) = \alpha_r(k).$$

The corresponding zeta function is given by

Definition 6. Let

$$Z_r(s) = \sum_{n=1}^{\infty} A_r(n) n^{-s} = \prod_{p \text{ prime}} F_r(p^{-s}).$$

We then get

Lemma 5. *One has that*

$$Z_r(s) = \prod_{m=1}^{k} \zeta(ms)^{\beta_r(m)} G_{k,r}(s),$$

where $G_{k,r}(s)$ is a Dirichlet series without real zeroes and absolutely convergent for $\mathrm{Re}(s) > 1/(k+1)$. Furthermore the $\beta_r(m)$'s are integers.

Proof. By Lemma 2 the result follows from Dahlquist [Dah52] with

$$\beta_r(m) = \sum_{d|m} \mu\left(\frac{m}{d}\right) \frac{d}{m} B_r(d), \tag{9}$$

where B_r comes from the expression

$$\log F_r(x) = \sum_{m=1}^{\infty} B_r(m) x^m.$$

Thus

$$\begin{aligned} G_{k,r}(s) &= \prod_{p \text{ prime}} F_r(p^{-s}) \prod_{m=1}^{k} (1 - p^{-ms})^{-\beta_r(m)} \\ &= \prod_{m=1}^{k} \zeta(ms)^{\beta_r(m)} Z_r(s) \end{aligned}$$

is without real zeroes and absolutely convergent for $\mathrm{Re}(s) > 1/(k+1)$. $\square$

With the notation $\beta(m) = \beta_m(m)$ we get from eq. (5) and the definition of the $\beta_r(m)$ eq. (9) that

$$\beta(m) = \beta_r(m). \qquad (r \geq m) \tag{10}$$

By using Definition 6, Lemma 5, eq (10) and Lemma 4 we obtain

Theorem 3. *One has that*

$$Z_1(s) = \zeta^2(s),$$
$$Z_2(s) = \frac{\zeta^2(s)\zeta^3(2s)}{\zeta(3s)},$$

and

$$Z_k(s) = \zeta^2(s)\zeta^3(2s)\zeta^3(3s)G_{3,k}(s), \qquad (k \geq 3)$$

where $G_{3,k}(s)$ is a Dirichlet series without real zeroes and absolutely convergent for $\mathrm{Re}(s) > 1/4$.

This implies the following result on average orders:

Corollary 3. *The number of subgroup classes of abelian groups of rank less than or equal to r and order atmost x is asymptotic to $C_r x \log x$ where C_r is a constant depending on r.*

5.2 The zeta function of subgroup classes of arbitrary rank

We now let $A(n) = \lim_{r\to\infty} A_r(n)$, $Z(s) = \lim_{r\to\infty} Z_r(s)$ and proceed as in the last section. We obtain with Lemma 2 and Dahlquist's theorem that

Lemma 6. *One has that*

$$Z(s) = \prod_{m=1}^{k} \zeta(ms)^{\beta(m)} G_k(s),$$

where $G_k(s)$ is a Dirichlet series without real zeroes and absolutely convergent for $\mathrm{Re}(s) > 1/(k+1)$*, and the $\beta(m)$'s are integers defined by eq.* (10).

which implies

Theorem 4. *Let $A(n)$ denote the number of subgroup classes of abelian groups of order n, and let*

$$Z(s) = \sum_{n=1}^{\infty} A(n) n^{-s}$$

denote the corresponding zeta function. Then

$$Z(s) = \zeta^2(s)\zeta^3(2s)\zeta^3(3s)G_3(s)$$

where $G_3(s)$ is a Dirichlet series without real zeroes and absolutely convergent for $\mathrm{Re}(s) > 1/4$*. Furthermore $Z(s)$ is a meromorphic function for* $\mathrm{Re}(s) > 0$ *and the imaginary axis is the natural boundary for $Z(s)$.*

Proof. That $\mathrm{Re}(s) = 0$ is the natural boundary follows from Lemma 2 which shows that F can not be written as a finite product $\prod_{j=1}^{k}(1-x^j)^{m_j}$. $\quad (m_j \in \mathbb{Z})$ and from Dahlquist's theorem the function cannot be meromorphically continued beyond the line $\mathrm{Re}(s) = 0$. $\square$

As before we get an estimate:

Corollary 4. *The number of subgroup classes of abelian groups of order atmost x is asymptotic to $Cx \log x$ where C is a constant.*

Remark 1. The constant C in Corollary 4 can be calculated by

$$C = \prod_{m=2}^{\infty} \zeta(m)^{\beta(m)} = 13.1854452968422695.$$

We notice that $\beta(m) \geq 0$ for $m = 1, \ldots, 12$ and for $k = 13$ Lemma 6 allows us to see (with the Mathematica program in the Appendix)

Remark 2. One has that

$$Z(s) = \zeta^2(s)\zeta^3(2s)\zeta^3(3s)\zeta^4(4s)\zeta^4(5s)\zeta^6(6s)\times \\ \times \zeta(7s)\zeta^4(8s)\zeta^6(9s)\zeta^2(10s)\zeta^{12}(12s)(\zeta(13s))^{-1}G_{13}(s),$$

where $G_{13}(s)$ is a Dirichlet series absolutely convergent for $\mathrm{Re}(s) > 1/14$ In particular this means that there are no poles for $Z(s)$ for $\mathrm{Re}(s) > 1/13$ except for $s = 1/k$, k integer. Under the Riemann hypothesis, we can use Lemma 6 with $k = 25$ to see that there are no poles for $Z(s)$ for $\mathrm{Re}(s) > 1/26$ except for $s = 1/k$, k integer.

For more calculations of $\beta(m)$ see the appendix where we use a Mathematica program to calculate its value for the first 100 values of m.

5.3 A question on the zeta function of subgroup classes of bounded rank

It seems likely that $r = 1$ and 2 are the only cases where $Z_r(s)$ has a meromorphic continuation to the entire complex plane. For higher rank we expect that

$Z_r(s)$ is a meromorphic function for $\mathrm{Re}(s) > 0$ with the imaginary axis as its natural boundary.

That $Z_r(s)$ has a meromorphic continuation to $\mathrm{Re}(s) > 0$ of course follows from Lemma 5. To prove that $\mathrm{Re}(s) = 0$ is the natural boundary we would have to show that $F_r(x)$ cannot be written as a finite product

$$F_r(x) = \prod_{j=1}^{k}(1 - x^j)^{m_j}. \qquad (m_j \in \mathbb{Z})$$

Thus it is sufficient to show that not all roots of the numerator of $F_r(x)$ lie on the unit circle which is easily verifiable by numerical calculation for small values of r. As an example, let $r = 3$. We can use the explicit form of $F_3(x)$ as given in the appendix, and see that the equation $1 + 2x + 2x^2 + x^3 + x^4 = 0$ has a root $x = -0.621744 + 0.440597i$ with an absolute value 0.762031.

Such calculations are not obvious for a general r.

6 Appendix

6.1 Tables

Table of $\beta_r(m)$																
$r \backslash m$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	2	3	-1	0	0	0	0	0	0	0	0	0	0	0	0	0
3	2	3	3	-1	-3	3	0	-2	0	0	6	-5	-6	6	1	9
4	2	3	3	4	-4	0	-3	2	9	-10	-2	-2	3	25	-25	11
5	2	3	3	4	2	-1	-6	-1	3	4	2	3	-12	-22	15	26
6	2	3	3	4	2	6	-7	-4	0	-2	1	13	10	-21	-4	-9
7	2	3	3	4	2	6	1	-5	-3	-5	-5	12	-1	8	17	-9
8	2	3	3	4	2	6	1	4	-4	-8	-8	6	-2	-3	18	20
9	2	3	3	4	2	6	1	4	6	-9	-11	3	-8	-4	7	21
10	2	3	3	4	2	6	1	4	6	2	-12	0	-11	-10	6	10
11	2	3	3	4	2	6	1	4	6	2	0	-1	-14	-13	0	9
12	2	3	3	4	2	6	1	4	6	2	0	12	-15	-16	-3	3
13	2	3	3	4	2	6	1	4	6	2	0	12	-1	-17	-6	0
14	2	3	3	4	2	6	1	4	6	2	0	12	-1	-2	-7	-3
15	2	3	3	4	2	6	1	4	6	2	0	12	-1	-2	9	-4
16	2	3	3	4	2	6	1	4	6	2	0	12	-1	-2	9	13

For the case of $\beta(m)$ we have the first 100 values: $\beta(1), \ldots, \beta(100) = 2$, 3, 3, 4, 2, 6, 1, 4, 6, 2, 0, 12, -1, -2, 9, 13, 0, -16, 6, 44, -25, -6, 16, -19, 52, -21, 52, -103, -140, 505, -203, -381, 286, 88, 185, -751, 564, 1015, -2304, 1007, 1876, -3432, 1177, 3665, -1582, -6119, -2558, 21792, -7745, -34936, 40625, 4248, -34948, 19176, -361, 30668, -104511, 81530, 196372, -457425, 148194, 497952, -459549, -261973, 163195, 1015378, -808365, -1895457, 3467251, -483924, -4303223, 4879125, 535751, -4991204, -634706, 7525125, 7551313, -31891601, 10748210, 53812155, -65485063, -16092470, 74326725, -12532241, -51617936, -53724288, 219808510, -91391802, -403364243, 663219049, -34111622, -908127917, 645523852, 643374980, -402710571, -1752056675, 1385661209, 3632651805, -6352203822, -317398867

6.2 Mathematica Programs

We can now implement the recursion formulae in Mathematica.

```
Clear[F];
F[0,x_,y_] := F[0,x,y]=1/(1-y)^2;
F[r_,x_,y_]:= F[r,x,y] =
   Factor[(x^r F[r-1,x,x^r]-F[r-1,x,y] y)/((x^r-y)(1-y))];
```

Now using

```
F_r(x)=F[r,x,0]
```

gives us for $r = 0, 1, 2, 3$ that

$$
\begin{aligned}
F_0(x) &= 1,\\
F_1(x) &= \frac{1}{(-1+x)^2},\\
F_2(x) &= \frac{1+x+x^2}{(-1+x)^4(1+x)^3},
\end{aligned}
$$

and

$$
F_3(x) = \frac{\left(1+2x+2x^2+x^3+x^4\right)\left(1+x+2x^2+2x^3+x^4\right)}{(-1+x)^6(1+x)^3(1+x+x^2)^4}.
$$

The program above is slow if we just want to calculate the lower order coefficients $\alpha_r(n)$ in the power series of $F_r(x)$, so the program we used to calculate the Table of $\beta_r(m)$ is the following (in this case with $m = 16$) :

```
Clear[a];
a[r_,n_,-1]:=a[r,n,-1]= 0;
a[0,n_,j_]:= a[0,n,j] = If[n==0,j+1,0];
a[r_,n_,j_]:=a[r,n,j]=a[r,n,j-1]+Sum[a[r-1,n-m r,m+j],
             {m,0,Floor[n/r]}];
a[r_,n_]:=a[r,n]=a[r,n,0];

m=16; Table[aa=Series[Log[Sum[a[r,j]*x^j,{j,0,m}]],{x,0,m}][[3]];
Table[ b=Divisors[n];
Sum[MoebiusMu[b[[j]]]/b[[j]] aa[[n/b[[j]]]],{j,1,Length[b]}],
{n,1,m}],{r,1,m}]
```

A similar program is used to calculate the $\beta(m)$ for $m = 1, \ldots 100$.

References

[Bho93] Gautami Bhowmik. Average orders of certain functions connected with arithmetic of matrices. *J. Indian Math. Soc. (N.S.)*, 59(1-4):97–105, 1993.

[BR98] Gautami Bhowmik and Olivier Ramaré. Algebra of matrix arithmetic. *J. Algebra*, 210(1):194–215, 1998.

[But87] Lynne M. Butler. A unimodality result in the enumeration of subgroups of a finite abelian group. *Proc. Amer. Math. Soc.*, 101(4):771–775, 1987.

[Cal03] C. Calderón. Asymptotic estimates on finite abelian groups. *Publ. Inst. Math. (Beograd) (N.S.)*, 74(88):57–70, 2003.

[Coh60] E. Cohen. On the average number of direct factors of a finite abelian group. *Acta Arith.*, 6:159–173, 1960.

[Dah52] Germund Dahlquist. On the analytic continuation of Eulerian products. *Ark. Mat.*, 1:533–554, 1952.

[ES34] P. Erdős and G. Szekeres. Über die Anzahl der Abelschen Gruppen gegebener Ordnung und über ein verwandtes zahlentheoretisches Problem. *Acta Szeged*, 7:95–102, 1934.

[GLP04] Dorian Goldfeld, Alexander Lubotzky, and László Pyber. Counting congruence subgroups. *Acta Math.*, 193(1):73–104, 2004.

[Kno85] John Knopfmacher. Solomon's zeta function and enumeration of lattices over orders. *Analysis*, 5(1-2):29–42, 1985.

[Krä88] Ekkehard Krätzel. On the average number of direct factors of a finite abelian group. *Acta Arith.*, 51(4):369–379, 1988.

[Mac79] I. G. Macdonald. *Symmetric functions and Hall polynomials*. The Clarendon Press Oxford University Press, New York, 1979. Oxford Mathematical Monographs.

[Men95] Hartmut Menzer. On the average number of direct factors of a finite abelian group. *J. Théor. Nombres Bordeaux*, 7(1):155–164, 1995. Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993).

[Wu00] Jie Wu. On the average number of direct factors of a finite abelian group. *Monatsh. Math.*, 131(1):79–89, 2000.

[Zha00] Wenguang Zhai. On the average number of unitary factors of finite abelian groups. II. *Acta Math. Sin. (Engl. Ser.)*, 16(4):549–554, 2000.